(19) World Intellectual Property Organization International Bureau





(43) International Publication Date 11 July 2002 (11.07.2002)

PCT

(10) International Publication Number WO 02/054663 A3

(51) International Patent Classification⁷: H04Q 7/38, H04L 9/32, 29/06

(21) International Application Number: PCT/US01/50643

(22) International Filing Date:

27 December 2001 (27.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/755,660 5 January 2001 (05.01.2001) US

- (71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).
- (72) Inventors: QUICK, Roy, Franklin, Jr.; 4502 Del Monte Avenue, San Diego, CA 92107 (US). ROSE, Gregory, G.; 6 Kingston Avenue, Mortlake, NSW 2137 (AU).

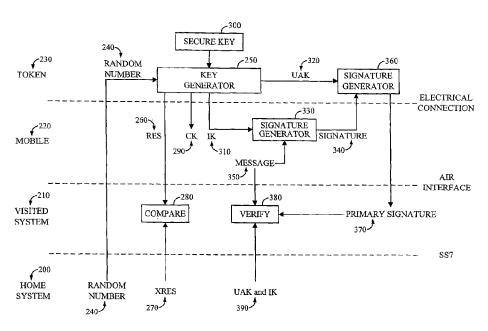
- (74) Agents: O'CONNELL, Robert, J. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

with international search report

[Continued on next page]

(54) Title: LOCAL AUTHENTICATION IN A COMMUNICATION SYSTEM



(57) Abstract: Methods and apparatus are presented for providing local authentication of subscribers travelling outside their home systems. A subscriber identification token (230) provides authentication support by generating a signature (370) based upon a key that is held secret from a mobile unit (220). A mobile unit (220) that is programmed to wrongfully retain keys from a subscriber identification token (230) after a subscriber has removed his or her token is prevented from subsequently accessing the subscriber's account.



(88) Date of publication of the international search report: 23 January 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/50643

A. CLASSI IPC 7	FICATION OF SUBJECT MATTER H04Q7/38 H04L9/32 H04L29/0	06		
According to	o International Patent Classification (IPC) or to both national classific	ation and IPC		
	SEARCHED	and and and	· · 	
	ocumentation searched (classification system followed by classification	on symbols)		
Documentat	ion searched other than minimum documentation to the extent that s	such documents are included in the fields se	earched	
Electronic d	ata base consulted during the international search (name of data ba	se and, where practical, search terms used)	
EPO-In	ternal			
C. DOCUME	ENTS CONSIDERED TO BE RELEVANT			
Category °	Citation of document, with indication, where appropriate, of the rel	evant passages	Relevant to claim No.	
A	"Rouges MS_Shell Treat Analysis" 3GPP TSG SA WG3 SECURITY, 'Onlir 28 - 30 November 2000, pages 1-1 XP002210348 Sophia Antipolis, France Retrieved from the Internet: <url:http: 2000_meetings="" docs="" ftp="" pdf="" s3-000711.pdf="" tsg_curity="" tsgs3_16_sopolis="" www.3gpp.org=""> 'retrieved on 2002-08-20! paragraph '02.2! paragraph '2.4.4! paragraph '05.2!</url:http:>	ne! 17, _sa/WG3_Se	6-9 1-5, 10-20	
X Furth	ner documents are listed in the continuation of box C.	Patent family members are listed	in annex.	
Special categories of cited documents: The later document published after the international filing date.				
T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published after the international filing date but *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention cannot be considered novel or cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.		the application but laimed invention be considered to sument is taken alone laimed invention rentive step when the re other such doou—		
P document published prior to the international filing date but later than the priority date claimed in the art. *A* document member of the same patent family			amily	
Date of the actual completion of the international search 20 August 2002 Date of mailing of the international search report 05/09/2002		rch report		
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–3016 Fax: (+31–70) 340–3016		Authorized officer Figiel, B		

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/50643

(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
tegory ° Citation of docume	nt, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Multiple Verifica BOGAZICI XP002210 Istanbu Retrieve <url:htt .trzsz{1="" 25="" abstract<="" cs="" re-based="" rs="" td=""><td>d from the Internet: p://citeseer.nj.nec.com/cache/pape 06/http:zSzzSzmercan.cmpe.boun.edu evizSzbas98.pdf/a-multiple-signatu .pdf> 'retrieved on 2002-08-20!</td><td>1,10,16, 211</td></url:htt>	d from the Internet: p://citeseer.nj.nec.com/cache/pape 06/http:zSzzSzmercan.cmpe.boun.edu evizSzbas98.pdf/a-multiple-signatu .pdf> 'retrieved on 2002-08-20!	1,10,16, 211
Systems' TIA/EIA/ - Novem Retrieve <url:htt g/imt2k/</url:htt 	IS-808, 'Online! ber 2000 (2000-11) XP002210350 d from the Internet: p://www.tiaonline.org/standards/sf cdma2000/TIA-EIA-IS-808.pdf> ed on 2002-08-20!	1,10,16, 21
MANAGEME PROPOSED PROCEEDI US, vol. 86, 1480-149 ISSN: 00	A ET AL: "MOBILITY AND SECURITY NT IN THE GSM SYSTEM AND SOME FUTURE IMPROVEMENTS" NGS OF THE IEEE, IEEE. NEW YORK, no. 7, July 1998 (1998-07), pages 7, XP000854168 18-9219 e document	1,10,16,